GitHub Actions Best Practices

Santosh Yadav
@SantoshYadavDev

About me

Senior Software Engineer @Celonis

GDE Angular, Nx Champion

GitHub Star

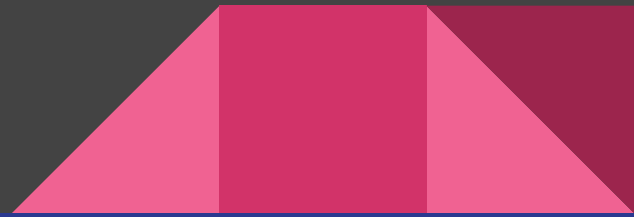
Co-Founder This Is Learning

Co-host This is Tech Talks

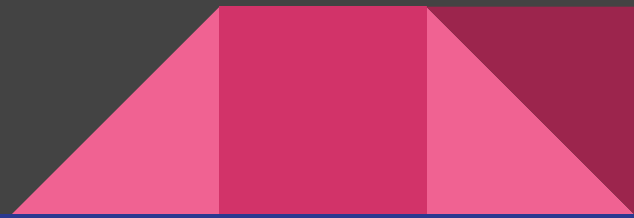
@SantoshYadavDev

Santosh Yadav
@SantoshYadavDev

What is GitHub Actions



Build tool to Automate your workflows



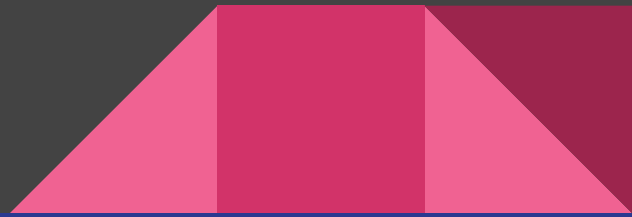
Run workflows on any GitHub event

Run workflow on major OS mac/windows/linux

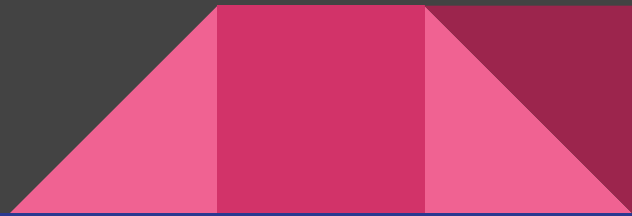
Supports Matrix

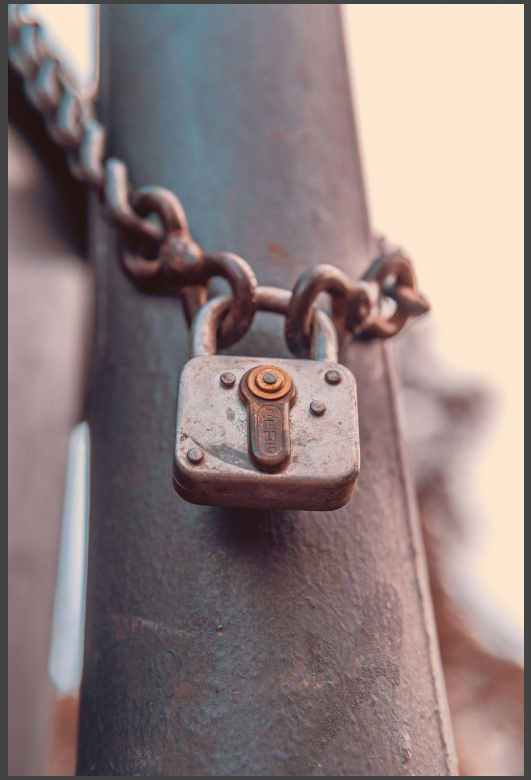
Write Custom Actions

Best practices starts from the day you create your organization

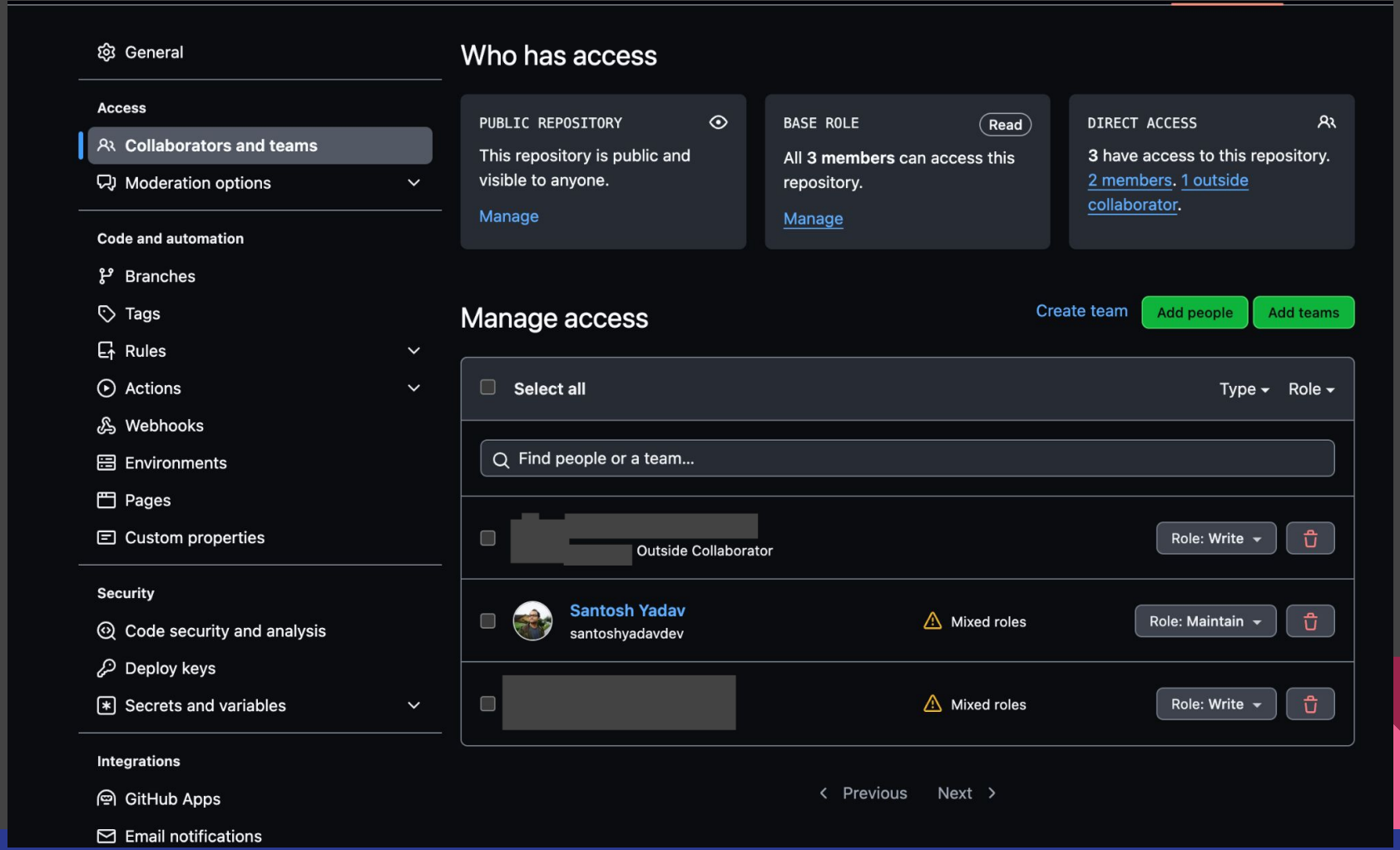


- Best practices starts from day one.
- Be proactive.
- Best practices changes with time.

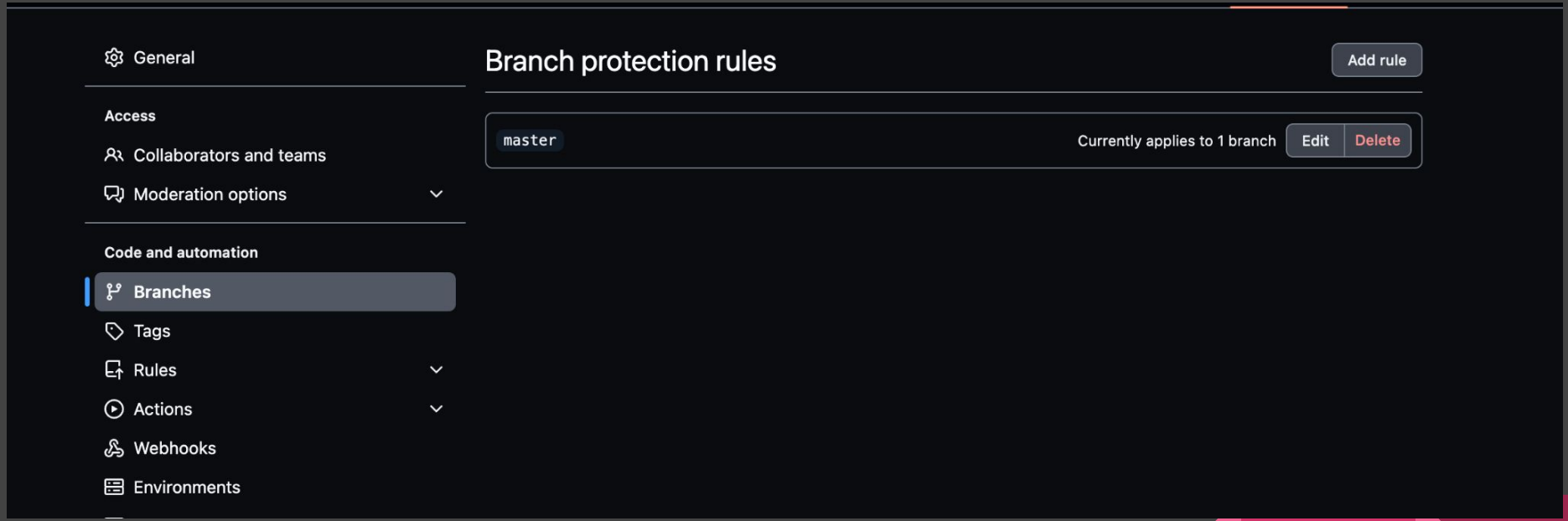




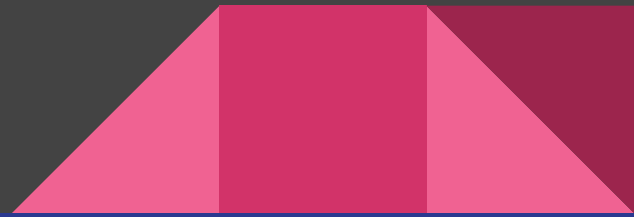
Give access to teams not individuals

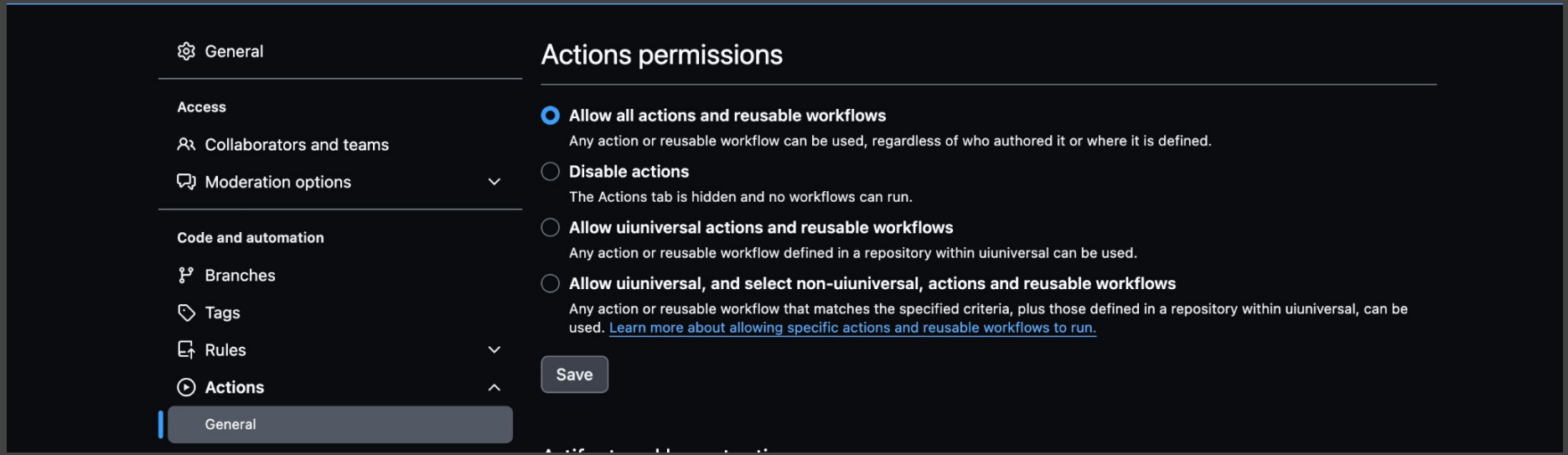

General
Access
Collaborators and teams
Moderation options
Code and automation
Branches
Tags
Rules
Actions
Webhooks
Environments
Pages
Custom properties
Security
Code security and analysis
Deploy keys
Secrets and variables
Integrations
GitHub Apps
Email notifications
Who has access
PUBLIC REPOSITORY
This repository is public and visible to anyone.
Manage
BASE ROLE
Read
All 3 members can access this repository.
Manage
DIRECT ACCESS
3 have access to this repository.
2 members. 1 outside collaborator.
Manage access
Create team
Add people
Add teams
Select all
Type
Role
Find people or a team...
Outside Collaborator
Role: Write
Santosh Yadav
santoshyadavdev
Mixed roles
Role: Maintain
Mixed roles
Role: Write
Previous
Next

Configure Branch Protection Rules

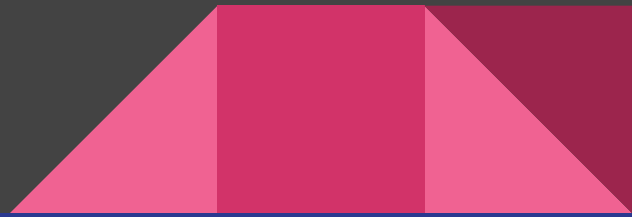

General
Access
Collaborators and teams
Moderation options
Code and automation
Branches
Tags
Rules
Actions
Webhooks
Environments
Branch protection rules
Add rule
master
Currently applies to 1 branch
Edit
Delete

Use Trusted Actions



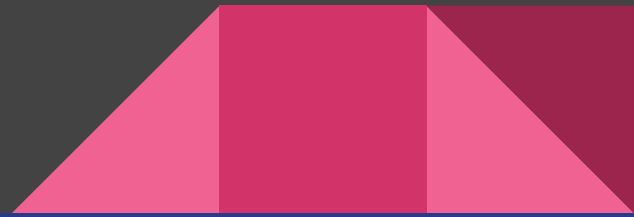

General
Access
Collaborators and teams
Moderation options
Code and automation
Branches
Tags
Rules
Actions
General
Actions permissions
Allow all actions and reusable workflows
Any action or reusable workflow can be used, regardless of who authored it or where it is defined.
Disable actions
The Actions tab is hidden and no workflows can run.
Allow uiuniversal actions and reusable workflows
Any action or reusable workflow defined in a repository within uiuniversal can be used.
Allow uiuniversal, and select non-uiuniversal, actions and reusable workflows
Any action or reusable workflow that matches the specified criteria, plus those defined in a repository within uiuniversal, can be used. Learn more about allowing specific actions and reusable workflows to run.
Save

Use Specific versions of Actions with SHA-1

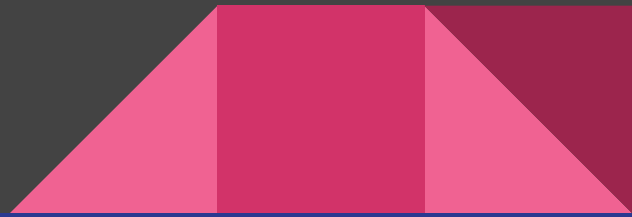


```yaml
# name of your workflow
name : build-workflow

# define events that trigger the workflow
on :
    push:
        branches:
        - main
    pull_request:
        branches:
        - main

# define jobs that run in the workflow
jobs:
    build:
        runs-on: ubuntu-latest
        steps:
        # checkout the repository
        - uses: actions/checkout@sha1
        # setup node with node version 16.x
        - name : Setup Npm
          uses: actions/setup-node@sha1
          with:
           node-version: '18.x'
           cache: 'npm'
        # Install node modules
        - name: Install node modules
          run: npm ci --force
        # Run build script
        - name: Run build
          run: npm run build
```

Audit 3rd party Actions.



Be careful with outside collaborators



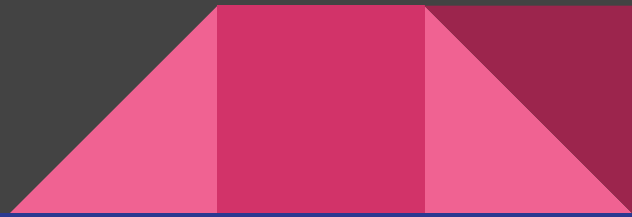
Fork pull request workflows from outside collaborators

Choose which subset of outside collaborators will require approval to run workflows on their pull requests. Learn more about approving workflow runs from public forks.

- ○ **Require approval for first-time contributors who are new to GitHub**
  Only first-time contributors who recently created a GitHub account will require approval to run workflows.
- ◉ **Require approval for first-time contributors**
  Only first-time contributors will require approval to run workflows.
- ○ **Require approval for all outside collaborators**

Save

Follow principle of least privilege for GITHUB_TOKEN



Workflow permissions

Choose the default permissions granted to the GITHUB_TOKEN when running workflows in this repository. You can specify more granular permissions in the workflow using YAML. Learn more about managing permissions.

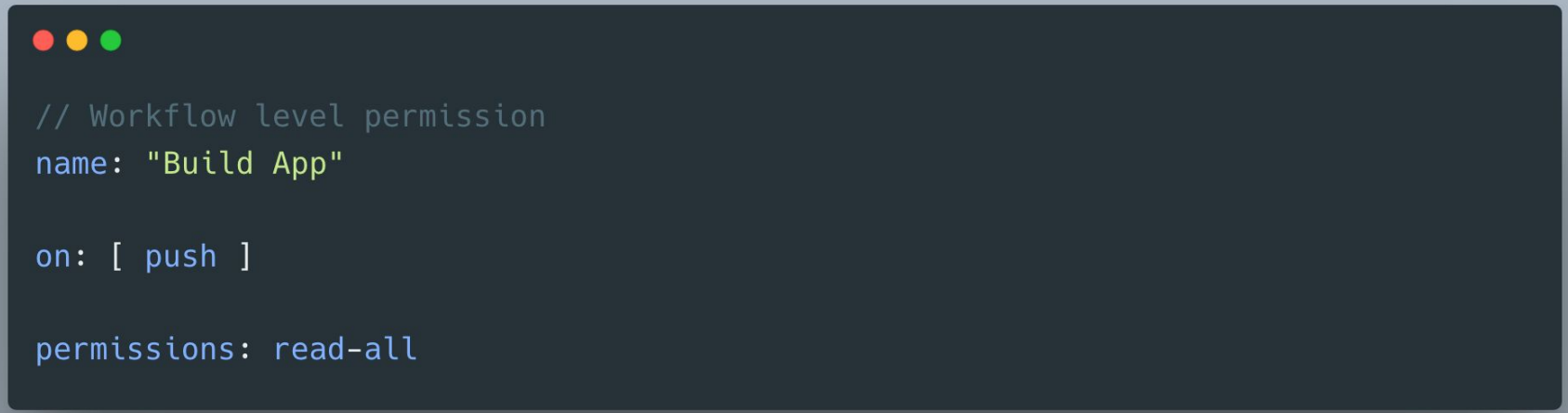
- ○ **Read and write permissions**
  Workflows have read and write permissions in the repository for all scopes.
- ◉ **Read repository contents and packages permissions**
  Workflows have read permissions in the repository for the contents and packages scopes only.

Choose whether GitHub Actions can create pull requests or submit approving pull request reviews.

- ☑ **Allow GitHub Actions to create and approve pull requests**

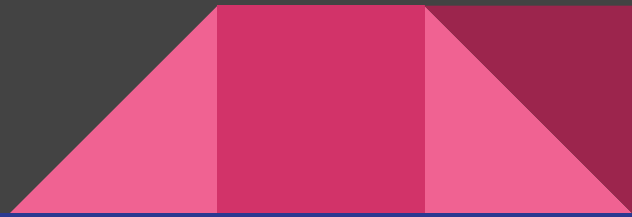
Save

```yaml
permissions:
  actions: read|write|none
  checks: read|write|none
  contents: read|write|none
  deployments: read|write|none
  id-token: read|write|none
  issues: read|write|none
  discussions: read|write|none
  packages: read|write|none
  pages: read|write|none
  pull-requests: read|write|none
  repository-projects: read|write|none
  security-events: read|write|none
  statuses: read|write|none
```

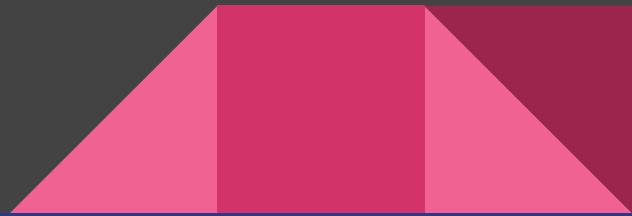

// Workflow level permission
name: "Build App"
on: [push]
permissions: read-all

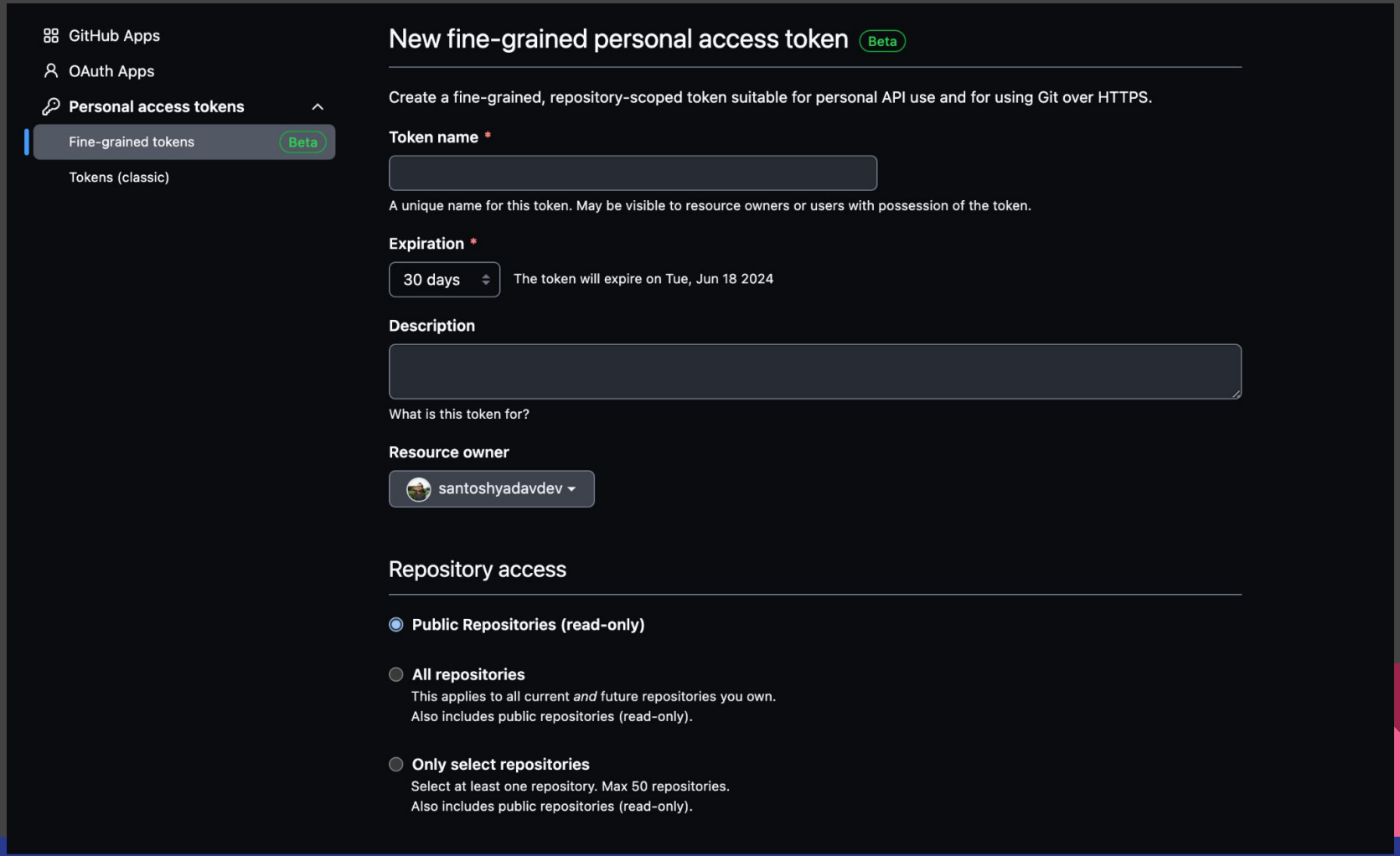
```yaml
jobs:
  release:
    runs-on: ubuntu-latest

    // job level permission
    permissions:
      packages: write
      pull-requests: write

    steps:
      - uses: actions/checkout@v4
```

Create environment level secrets.



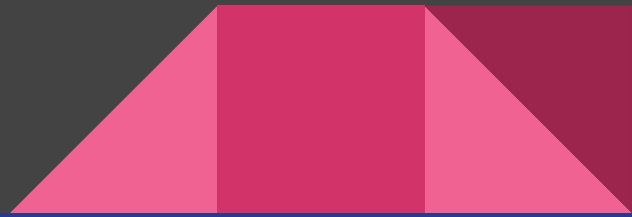
Personal Access Token



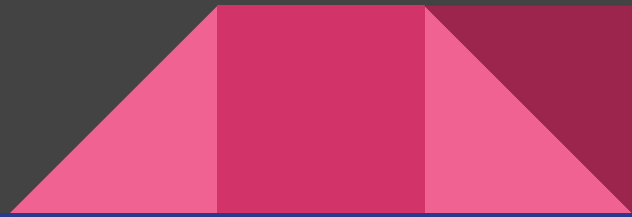

GitHub Apps
OAuth Apps
Personal access tokens
Fine-grained tokens
Beta
Tokens (classic)
New fine-grained personal access token
Beta
Create a fine-grained, repository-scoped token suitable for personal API use and for using Git over HTTPS.
Token name *
A unique name for this token. May be visible to resource owners or users with possession of the token.
Expiration *
30 days
The token will expire on Tue, Jun 18 2024
Description
What is this token for?
Resource owner
santoshyadavdev
Repository access
Public Repositories (read-only)
All repositories
This applies to all current and future repositories you own.
Also includes public repositories (read-only).
Only select repositories
Select at least one repository. Max 50 repositories.
Also includes public repositories (read-only).

Enable 2FA and SSO

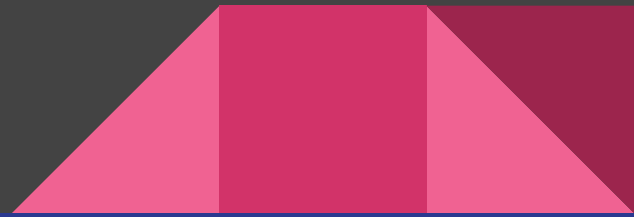
Register all secrets.



Rotate tokens and do planned audits.



Monitor permission for your action



```yaml
# name of your workflow
name : build-workflow

# define events that trigger the workflow
on :
    push:
        branches:
        - main

# define jobs that run in the workflow
jobs:
    build:
        runs-on: ubuntu-latest
        steps:
        # checkout the repository
        - uses: actions/checkout@v3
        # Check permissions
        - name: Check permissions
          uses: GitHubSecurityLab/actions-permissions/monitor@v1  --> monitor
action by GitHub Security
          with:
            config: ${{ vars.PERMISSIONS_CONFIG }}
```

Use GitHub token permissions Monitor and Advisor actions

https://github.com/GitHubSecurityLab/actions-permissions

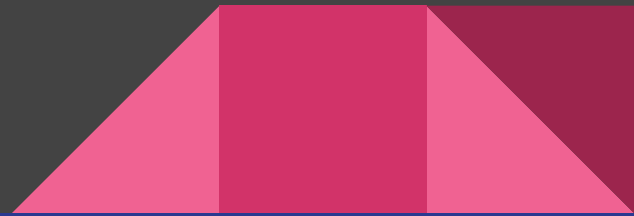
https://github.com/GitHubSecurityLab/actions-permissions/tree/main/advisor

References

- https://adnanthekhan.com/
- https://0xn3va.gitbook.io/cheat-sheets/ci-cd/github/actions#github-runner-registration-token-disclosure
- https://securitylab.github.com/research/github-actions-building-blocks/
- https://docs.github.com/en/actions

Thanks to my GitHub Sponsors

- Cometa.rocks
- Sunil
- Darshan
- Umair
- Anand



Thank you

Santosh Yadav
@SantoshYadavDev